PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-005384
(43)Date of publication of application : 12.01.2001

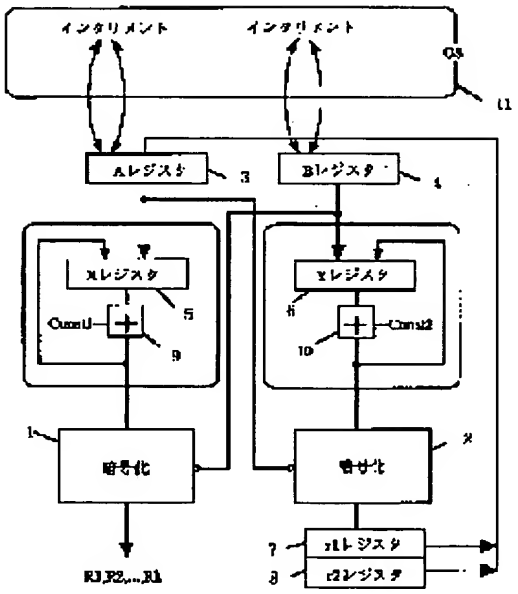
(51)Int.CI. G09C 1/00
G06F 7/58
G06K 19/073

(21)Application number : 11-177913
(22)Date of filing : 24.06.1999

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : MATSUZAKI NATSUME
ONO TAKATOSHI
MASAKI TADAKATSU
KAWANO SHINJI
NAKABE FUTOSHI
INOUE KAZUNORI

(54) RANDOM-NUMBER GENERATING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a safe random-number generating method at a low cost by providing the above system with a random-number updating section which determines the next kind according to the random number kind, and an operating system which updates the random number kind at arbitrary timing.
SOLUTION: A processing section 11 of the operating system forms a random- number system for a prescribed length by repeating a cipher section 1, while updating input by an X register 5 and an adder section 9 with the value of an A register 3 as an initial value. Output values are stored in an r1 register 7 and an r2 register 8 by repeating a Y register 6 and an adder section 10 with the value of a B register 4 as an initial value and are respectively stored in the A and B registers for the purpose of random-number generation of the next block. The operation system increments the A and B registers with arbitrary timings. Since a secret key cipher E which is the function originally disposed at an IC card and the operating system are utilized, additional hardware/ software is made few.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 7/58 — A1

(11) International Publication Number: WO 93/23804

(43) International Publication Date: 25 November 1993 (25.11.93)

(21) International Application Number: PCT/SE93/00414

(22) International Filing Date: 11 May 1993 (11.05.93)

(30) Priority data:
9201498-4 12 May 1992 (12.05.92) SE

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET LM ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)* : HOFVERBERG, Mikael [SE/SE]; Margaretavägen 14, S-175 35 Järfälla (SE).

(74) Agents: GRAUDUMS, Valdis et al.; Albihn West AB, Box 142, S-410 22 Göteborg (SE).

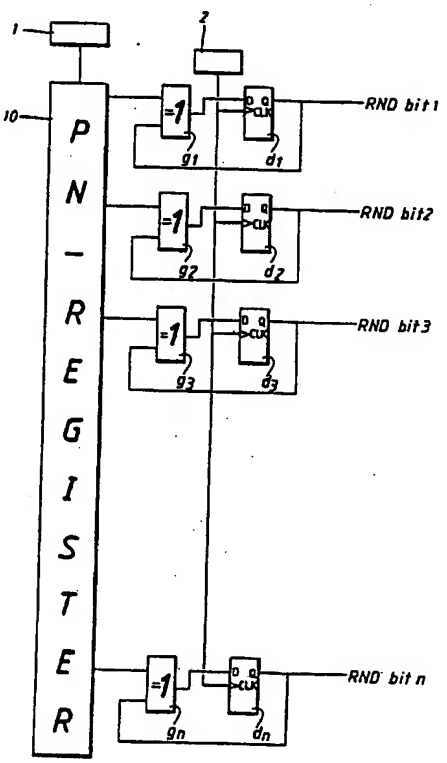
(81) Designated States: GB, JP, US.

Published
With international search report.

(54) Title: APPARATUS AND METHOD FOR RANDOM NUMBER GENERATION

(57) Abstract

The invention relates to an apparatus and a method for random number generation. The apparatus comprises a feedback shift register (10) which receives signals from a first signalling device, the shift register (10) further being connected to at least one delay device (d_1, ..., d_n). This or these delay device(s) deliver (each) a random number when receiving a clock signal from a second signalling device (2). The first signalling device (1) comprises a fast clock and the feedback shift register (10) is connected to the delay device(s) (d_1, ..., d_n) via at least one logical gate (g_1, ... g_n), the output(s) of delay device(s) (d_1, ..., d_n), being fed back to said gate(s) (g_1, ..., g_n), the second signalling device (2) delivering clock signals originating from external events.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	FR	France	MR	Mauritania
AU	Australia	GA	Gabon	MW	Malawi
BB	Barbados	GB	United Kingdom	NL	Netherlands
BE	Belgium	GN	Guinea	NO	Norway
BF	Burkina Faso	GR	Greece	NZ	New Zealand
BG	Bulgaria	HU	Hungary	PL	Poland
BJ	Benin	IE	Ireland	PT	Portugal
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SK	Slovak Republic
CI	Côte d'Ivoire	KZ	Kazakhstan	SN	Senegal
CM	Cameroon	LI	Liechtenstein	SU	Soviet Union
CS	Czechoslovakia	LK	Sri Lanka	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	MC	Monaco	UA	Ukraine
DK	Denmark	MG	Madagascar	US	United States of America
ES	Spain	ML	Mali	VN	Viet Nam
FI	Finland	MN	Mongolia		

TITLE

Apparatus and method for random number generation

TECHNICAL FIELD

The present invention relates to an apparatus for random number generation comprising a feedback shift register which receives signals from a first signalling device, the feedback shift register being connected to at least one clocked delay device which upon receiving a clock signal from a second signalling device produces a random number. Such devices find e.g. their use within radiocommunication, for production of crypto-keys etc. The requirements that random numbers, both random numbers produced by one and the same apparatus as well as random numbers produced by different apparatuses are as uncorrected and unpredictable as possible.

There is furthermore often a need of a random number generator which may be integrated in an LSI (Large Scale Integration)-circuit.

STATE OF THE ART

An apparatus of the abovementioned kind is given by US-A-4 905 176. In this known apparatus On-Chip noise-sources are used as a first signalling device. Such On-Chip noise sources are both difficult and expensive to fabricate. Moreover they consume much current. Furthermore the random numbers which are generated by this apparatus do not originate from external events but depend on parameters of the LSI such as for example material and constitution, the

circumstances prevailing at its fabrication and so on. Since the random numbers come directly from the outputs of a large PN-register, in case a such is used, different apparatuses which are started up and driven simultaneously will generate the same random number. Moreover, different inputs from the same PN sequence are used as the input to the logical gate (XOR). A further inconvenience with this apparatus is that the random numbers merely can be obtained in series and not parallelly.

In other known apparatuses noise diodes are used which generate noise which is amplified and quantified. In this manner generated random numbers are read by a computer. Random number generators of this kind require a large number of discrete and integrated components and it is furthermore not possible to integrate the whole random number generator in an LSI. Furthermore these apparatuses require high voltages, such as approximately 20 V as well as high currents, e.g. more than 50 mA.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide an apparatus for generation of random numbers which give as good and uncorrolated random numbers as possible, and wherein different apparatuses produce different random numbers. It is furthermore an object of the invention to provide an apparatus which do not require high currents and which only requires a low voltage. Preferably the apparatus consumes less that 1 mA and merely requires about 5 V. A further object of the invention is to provide a random number generator which is entirely digital, easy to integrate, particularly in an LSI, and which can be fabricated in a cheap way and by cheap components.

These objects as well as others are achieved through an apparatus of the aforementioned kind wherein the first signalling device comprises a fast clock, the feedback shift register is connected to the delay device/devices via at least one logical gate, the output(s) delay device(s) further being fed back to said date/gates, and wherein clocking signals from the second signalling device originate from external events.

It is also an object of the invention to provide a method for generation of random numbers by which the in the foregoing mentioned objects are achieved.

The objects are achieved through a method wherein a random number generated by one apparatus is independent of a random number simultaneously generated by another apparatus, wherein a PN-register receives a clocking signal from a first signalling device, the PN-register being connected to at least one delay device, preferably a D-flip-flop which from a second signalling device receives an asynchronous, external signal and which thereupon produces a random number, wherein the data entrance of the delay device is connected to the PN-register via a logical gate, preferably an XOR-gate, the output from the delay device furthermore being fed back to the XOR-gate(s), and the fast clock delivering signals with a clocking frequency f_1 which essentially exceeds the clocking frequency f_2 of the second signalling device and parallelly delivering of clock signals to the delay devices from the second signalling device.

Preferred embodiments are given by the characteristics in the subclaims.

The feedback shift register preferably comprises a so called PN-register, i.e. Pseudo-Noise-register. This PN-register particularly receives signals from the first signalling device comprised by a fast clock. Particularly this fast clock has a clocking frequency which is so high that the PN-register manages to wraparound between each clock signal delivered by the second signalling device which produces signals for the delay device(s). For an 18-bit PN-register the frequency may according to a preferred embodiment e.g. be about 1 MHz. In this case the register wraps around about four times per second. Preferably the logical gate/gates are so called XOR-gates. Particularly, the output thereof is connected to the data-entrance of a D-type flip-flop the Q-output of which in turn is fed back to the logical gate. Through a feedback coupling of this kind the random number will depend on what has happened in the preceding step which in turn depends on the preceding step etc.

According to a preferred embodiment the apparatus comprises a number of clocked delay devices d_i (i = 1, ..., n) connected in parallel for parallel generation of (i = 1, ..., n) random numbers. Particularly at least a number of bit positions of the feedback shift register may be connected each to a separate logical gate, the ouput of each logical gate being connected to a separate clocked delay device, especially a D-type flip-flop, furthermore each delay device or D-flip-flop being fed back to its respective logical gate (XOR-gate) and the delay devices being parallely connected to the second signalling device for obtaining external, asynchronous signals. These signals come from external events from outside the apparatus that comprised by the random number generator, for example from the keyboard of the computer, if the keyboard is seen as an external device or through the RS-232-interface or similar.

It may also be an asynchronus communication with other units or similar; it being essential that the signals originate form external events. Therethrough a random number is produced which differs from one apparatus to another apparatus even it produced simultaneously. The apparatus is more particularly so constructed that it easily can be integrated in an LSI-circuit.

DESCRIPTION OF THE DRAWINGS

The invention will in the following be further described by reference to the accompanying drawings, which are given for explanatory, by no means limiting, purposes, wherein

Fig. 1 shows a block diagram of an apparatus for parallel generation of a number of random numbers according to the invention,

Fig. 2 shows a system comprising an apparatus for generation of random numbers according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The apparatus for random number generation according to Fig. 1 comprises a feedback PN-shift register 10. This PN-register receives signals from a fast clock 1. In the shown embodiment each bit position in the PN-register 10 is connected an XOR-gate (g_1, g_2, ..., g_n). The output of each XOR-gate(g_1, ..., g_n) is connected to the data-entrance D of a delay device (d_1, ..., d_n). The "Q"-output (non-inverting) of the delay device (d_1, ..., d_n), e.g. a D-flip-flop is fed back via a feedback loop to the corresponding logical gate (g_1, ..., g_n). The D-flip-flops or delay devices d_1, ..., d_n are connected in parallel to a second signalling device 2 from which they receive an asynchronus, external signal. The events or signals from this second signalling device 2

originate from external, asynchronus events taking place outside the apparatus for random number generation itself. These events may e.g. come from asynchronus communication with other units, through the RS-232-interface etc. Since the frequency of the first signalling device 1, i.e. the fast clock is so high that the PN-register 10 manages to wraparound at least once between each signal from the second signalling device 2, very good, to the greatest extent uncorrolated random numbers i, i = 1, 2, ..., n) (RND bit 1, RND bit 2, ..., RND bit n) are obtained at the Q-output of the respective D-flip-flop d_1, ..., d_n. If an 18-bit PN-register is used, the clocking frequency of the fast clock on the first signalling device 1 may be around 1 MHz which would mean that the PN-register wraps around about four times a second. The delay devices d_1, ..., d_n (the D-flip-flops) produce a random number each time a signal is received from the second signalling device 2. Since the events delivered from the second signalling device have an external origin i.e. come from outside the probability that two arrangements comprising an apparatus for random number generation would generate the same random number is minimal.

In Fig. 2 an example of a system comprising an apparatus for random number generation according to the invention is shown, the random numbers being fed to a micro processor with a number of external interfaces, a keyboard and a random number generator, D-bus meaning data-bus and A-bus meaning address-bus. The IRQ-signals (interruption request) from the external interface and the keyboard generate a signal "event" which was described above. The fast clock is for example generated by an external oscillator, osc.

The invention shall of course not be limited to the shown embodiments but can be freely varied within the scope of the claims, for example is it possible to, for certain applications, merely have one delay device and one gate respectively for obtaining one random number whereas in other applications a number of parallel random numbers are required. Furthermore the PN-register does not necessarily have to be an 18-bit register etc.

Claims

1. Apparatus for random number generation comprising a feedback shift register (10) which receives signals from a first signalling device (1), the feedback shift register (10) being connected to at least one clocked delay device (d_1, ..., d_n) which upon receiving a clock signal from a second signalling device (2) produces a random number, c h a r a c t e r i z e d in that the first signalling device comprises a fast clock, that the feedback shift register (10) is connected to the delay device/devices (d_1, ..., d_n) via at least one logical gate (g_1, ..., g_n), the output(s) of the delay device(s) (d_1, ..., d_n) further being fed back to said gate/gates (g_1, ..., g_n), the clock signals from the second signalling device (2) originating from external events.

2. Apparatus according to claim 1, c h a r a c - t e r i z e d in that the clock signals from the second signalling device (2) originate from asynchronous, external events.

3. Apparatus for random number generation according to claim 1, c h a r a c t e r i z e d in that the feedback shift register (10) comprises a so called PN-register.

4. Apparatus according to claim 3, c h a r a c t e r i z e d in that the logical gate (g_1, ..., g_n) comprises an XOR-gate.

5. Apparatus according to claim 4, c h a r a c - t e r i z e d in that the delay device (d_1, ..., d_n) comprises a type D-flip-flop.

6. Apparatus according to any one of the preceding claims, c h a r a c t e r i z e d in that it comprises a number of delay devices d_i (i = 1, ..., n) connected in parallel for generation of i (i = 1, ..., n) random numbers parallelly.

7. Apparatus according to claim 6, c h a r a c - t e r i z e d in that at least a number of bit-positions of the feedback shift register (10) are connected to each a separate logical gate (g_1, ..., g_n), the output of each gate being connected to a separate clocked delay device (d_1, ..., d_n), the output of each delay device (d_1, ..., d_n) furthermore being fed back to its respective logical gate (g_1, ..., g_n) the delay devices (d_1, ..., d_n) being parallely connected to the second signalling device (2) for receiving of external, asynchronus signals.

8. Apparatus according to anyone of claims 1-5, c h a r a c t e r i z e d in that the fast clock (1) has a clocking frequency f_1, which essentially exceeds the clocking frequency, f_2, of the second signalling device (2) so that the PN-register (10) wraps around at least once between two consecutive clocking signals from the second signalling device (2).

9. Apparatus according to claim 7, c h a r a c - t e r i z e d in that the fast clock (1) has a clocking frequency f_1, which essentially exceeds the clocking frequency, f_2, of the second signalling device (2) so that the PN-register (10) wraps around at least once between two consecutive clocking signals from the second signalling device (2).

10. Apparatus according to claim 9, c h a r a c - t e r i z e d in that the PN-register (10) is an 18-bits PN-register and that the clocking frequency, f_1, of the first signalling device (1) is about 1 MHz.

11. Apparatus for random number generation according to anyone of claims 1-5, c h a r a c t e r i z e d in that it is integrated in an LSI-circuit.

12. Apparatus for random number generation according to claim 7, c h a r a c t e r i z e d in that it is integrated in an LSI-circuit.

13. Apparatus for random number generation according to claim 5, c h a r a c t e r i z e d in that the data entrance of the delay device(s) (d_1, ..., d_n) being connected to the PN-register (10) via XOR-gates, the output of the delay device (d_1, ..., d_n) further being connected to an XOR-gate (g_1, ..., g_n) via a feedback loop, the second signalling device parallelly delivering clocking signals to a number of delay devices.

14. Apparatus for random number generation according to claim 7, c h a r a c t e r i z e d in that the data entrance of the delay device(s) (d_1, ..., d_n) being connected to the PN-register (10) via XOR-gates, the output of the delay device (d_1, ..., d_n) further being connected to an XOR-gate (g_1, ..., g_n) via a feedback loop, the second signalling device parallelly delivering clocking signals to a number of delay devices.

15. Method for random number generation wherein a random number generated by one apparatus is independent of a random number simultaneously generated by another apparatus, wherein a PN-register (10) receives a clocking signal

from a first signalling device (1), the PN-register (10) being connected to at least one delay device (d_1, ..., d_n), preferably a D-flip-flop, which from a second signalling device (2) receives an asynchronus, external signal and which thereupon produces a random number, c h a r a c - t e r i z e d in that the data entrance of the delay device (d_1, ..., d_n) is connected to the PN-register (10) via a logical gate (g_1, ..., g_n), preferably an XOR-gate, the output from the delay device (d_1, ..., d_n) furthermore being fed back to the XOR-gate(s) (g_1, ..., g_n), and the fast clock (1) delivering signals with a clocking frequency f_1 which essentially exceeds the clocking frequency f_2 of the second signalling device (2) and parallelly delivering clock signals to the delay devices (d_1, ..., d_n) from the second signalling device (2).

16. Method according to claim 15, c h a r a c - t e r i z e d in that the frequency, f_1, of the fast clock (1) is so high that the PN-register (10) wraps around at least once between each signal delivered from the second signalling device (2).

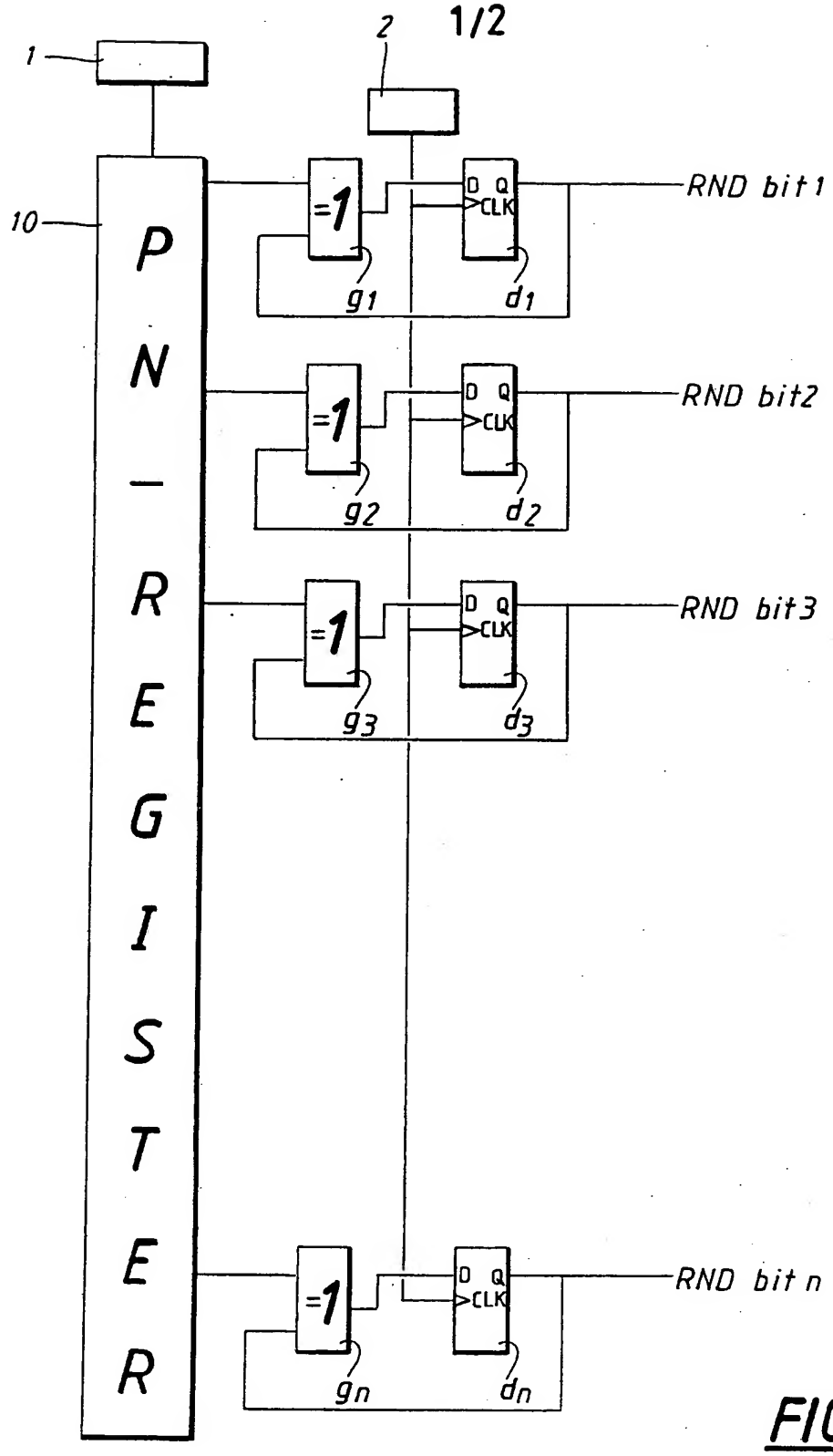

1
2
10
P
N
-
R
E
G
I
S
T
E
R
=1
D Q
CLK
g1
d1
RND bit1
g2
d2
RND bit2
g3
d3
RND bit3
gn
dn
RND bit n

FIG.1

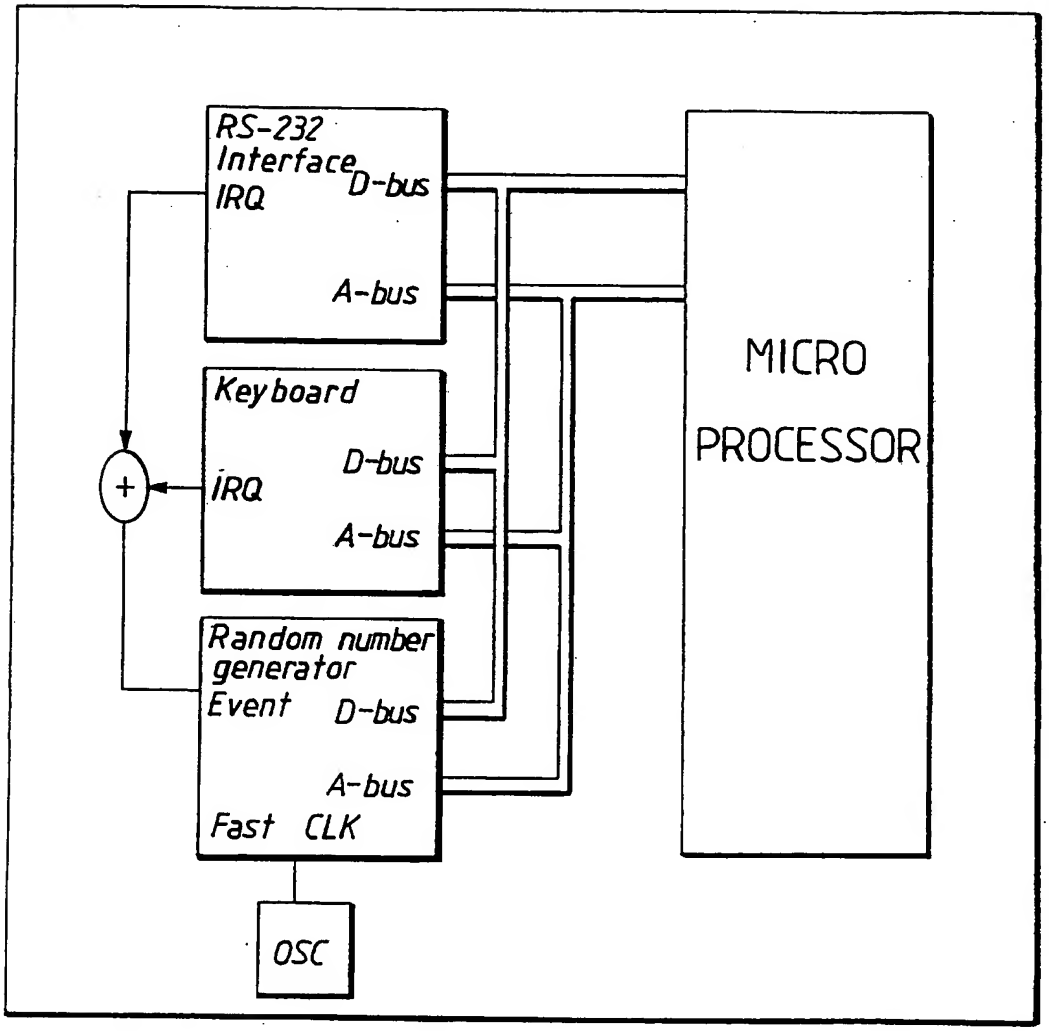

RS-232
Interface
IRQ
D-bus
A-bus
Keyboard
IRQ
D-bus
A-bus
Random number
generator
Event
D-bus
A-bus
Fast CLK
OSC
MICRO
PROCESSOR

FIG.2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 93/00414

A. CLASSIFICATION OF SUBJECT MATTER

IPC5: G06F 7/58
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC5: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG: 340, 350, 351

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4905176 (RAYMOND A. SCHULZ), 27 February 1990 (27.02.90), column 2, line 5 - column 3, line 10, figure 4 --	1-16
A	IBM Technical Disclosure Bulletin, Volume 30, No 11, April 1988, . , "INTEGRATED CIRCUIT COMPATIBLE RANDOM NUMBER GENERATOR" page 333 - page 335 --	1-16
A	IEE PROCEEDINGS-E, Volume 138, No 3, May 1991, J. Saarinen, J. Tomberg, L. Vehmanen, Prof. K. Kaski, "VLSI implementation of Tausworthe random number generator for parallel processing environment" page 138 - page 146 --	1-16

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 1993	27 -07- 1993
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Katarina Fredriksson Telephone No. +46 8 782 25 00